



PERANCANGAN DAN IMPLEMENTASI SISTEM KEAMANAN JARINGAN SMART GRID

Rakhmadi Rahman^a, Putri Dyananda Luqman^{b*}

^a Fakultas Sains / Sistem Informasi, Institut Teknologi Bacharuddin Jusuf Habibie, Parepare Sulawesi Selatan

^b Fakultas Sains / Sistem Informasi, putridyananda@gmail.com, Institut Teknologi Bacharuddin Jusuf Habibie, Parepare Sulawesi Selatan

* Korespondensi

ABSTRACT

In the era of digitalization, smart grids have become vital for efficient and sustainable energy distribution but are vulnerable to various cyber threats. This research aims to design and implement a robust network security system for smart grids to protect critical infrastructure from cyber-attacks. The methodology involves risk analysis, threat model development, and the application of advanced encryption and authentication technologies. The proposed security system incorporates multiple layers of protection, including firewalls, intrusion detection systems (IDS), and incident response mechanisms, supplemented by blockchain-based security protocols to ensure data integrity. Implementation results demonstrate that the system can effectively identify and counteract cyber threats, enhancing network resilience. Performance testing indicates that despite the additional security layers, the system operates within acceptable limits for latency and throughput. This research significantly contributes to the development of security standards for smart grids and provides practical recommendations for the industry in designing reliable and efficient security systems.

Keywords: Smart grid, network security, blockchain, cryptography, prototype.

Abstrak

Dalam era digitalisasi, smart grid menjadi solusi vital untuk distribusi energi yang efisien dan berkelanjutan, namun rentan terhadap berbagai ancaman siber. Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem keamanan jaringan yang tangguh bagi smart grid guna melindungi infrastruktur kritis dari serangan siber. Metodologi yang digunakan mencakup analisis risiko, pengembangan model ancaman, serta penerapan teknologi enkripsi dan autentikasi canggih. Sistem keamanan yang diusulkan melibatkan beberapa lapisan proteksi seperti firewall, sistem deteksi intrusi (IDS), dan mekanisme respons insiden, ditambah penerapan protokol keamanan berbasis blockchain untuk menjaga integritas data. Hasil implementasi menunjukkan bahwa sistem ini mampu mengidentifikasi dan menangkal serangan secara efektif, dengan peningkatan resiliensi jaringan terhadap ancaman. Pengujian performa juga mengindikasikan bahwa meskipun ada penambahan lapisan keamanan, sistem tetap beroperasi dalam batasan yang dapat diterima untuk latency dan throughput. Penelitian ini memberikan kontribusi penting dalam pengembangan standar keamanan untuk smart grid dan menawarkan rekomendasi praktis bagi industri dalam merancang sistem keamanan yang andal dan efisien.

Kata Kunci: Smart grid, keamanan jaringan, blockchain, kriptografi, prototype.

1. PENDAHULUAN

Smart Grid merupakan evolusi dari jaringan listrik tradisional dengan memanfaatkan teknologi informasi dan komunikasi untuk mengoptimalkan produksi, distribusi, dan konsumsi energi. Keunggulan Smart Grid meliputi efisiensi yang lebih tinggi, integrasi sumber energi terbarukan, dan kemampuan untuk merespons permintaan energi secara dinamis. Namun, Smart Grid juga rentan terhadap ancaman keamanan siber yang dapat mengganggu operasional dan menyebabkan kerugian besar. Dengan semakin kompleksnya

infrastruktur energi yang terhubung, kebutuhan akan sistem keamanan yang kuat dan andal menjadi sangat mendesak. Jaringan Smart Grid tidak hanya mengandalkan teknologi konvensional tetapi juga melibatkan berbagai perangkat pintar, sensor, dan sistem kendali yang saling berinteraksi melalui internet dan jaringan komunikasi lainnya. Hal ini membuka celah bagi potensi serangan siber yang bisa merusak stabilitas dan keandalan jaringan listrik.

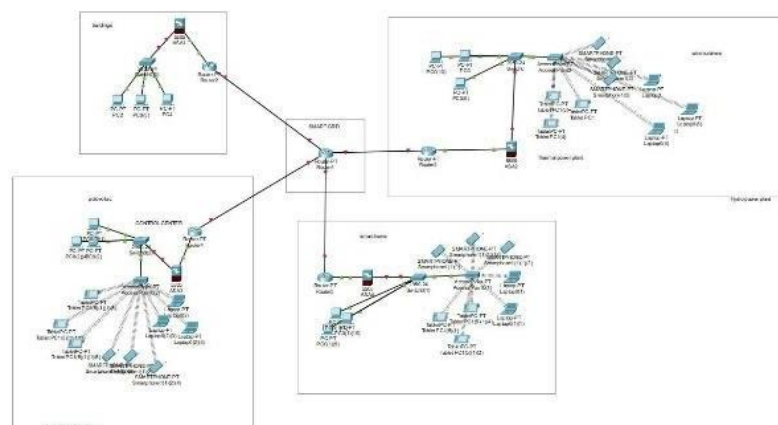
Oleh karena itu, perancangan arsitektur keamanan yang optimal untuk melindungi lalu lintas jaringan dan membatasi akses yang tidak sah menjadi sangat penting. Tantangan utama dalam merancang sistem keamanan untuk Smart Grid meliputi kebutuhan untuk memastikan integritas, kerahasiaan, dan ketersediaan data serta sistem kontrol yang digunakan dalam jaringan tersebut. Selain itu, sistem keamanan harus mampu mendeteksi dan merespons ancaman secara real-time untuk mencegah kerusakan yang lebih besar. Pendekatan yang komprehensif diperlukan untuk mengatasi tantangan ini, yang mencakup analisis risiko, perancangan arsitektur keamanan berlapis, implementasi teknologi keamanan canggih, serta pengujian dan evaluasi sistem secara berkala. Dengan demikian, tujuan dari penelitian ini adalah untuk mengembangkan dan mengimplementasikan sistem keamanan yang efektif dan efisien pada jaringan smart grid, guna memastikan operasional yang aman dan andal di tengah ancaman siber yang semakin meningkat.

2. METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif dan eksperimental untuk mengembangkan dan mengimplementasikan sistem keamanan jaringan Smart Grid. Tahap awal melibatkan analisis risiko untuk mengidentifikasi potensi ancaman dan kerentanan menggunakan penilaian risiko kualitatif dan kuantitatif serta metode Delphi yang melibatkan pakar keamanan siber dan Smart Grid. Berdasarkan hasil analisis ini, dirancang arsitektur keamanan dengan lapisan perlindungan seperti enkripsi, otentikasi, kontrol akses, serta deteksi dan mitigasi ancaman. Implementasi teknologi keamanan mencakup integrasi protokol enkripsi pada komunikasi data, penerapan otentikasi multifaktor, dan penggunaan firewall serta sistem deteksi dan pencegahan intrusi.

Pengumpulan data dilakukan melalui studi literatur, survei, kuesioner, observasi, wawancara, dan data eksperimental dari pengujian penetrasi dan evaluasi kinerja sistem keamanan. Data sekunder dikumpulkan dari sumber akademik dan industri, sementara data primer diperoleh dari pakar keamanan siber, pengelola jaringan listrik, dan pengguna Smart Grid. Proses pengembangan sistem keamanan meliputi identifikasi kebutuhan keamanan, desain dan simulasi, pembangunan prototipe, pengujian, iterasi untuk perbaikan, serta pelatihan dan dokumentasi bagi personel terkait. Dengan pendekatan ini, diharapkan sistem keamanan yang dirancang mampu melindungi jaringan Smart Grid dari ancaman siber dan memastikan operasional yang aman dan andal.

3. HASIL DAN PEMBAHASAN



Gambar 1. Desain Jaringan smart grid

Gambar 1 menjelaskan desain jaringan Smart Grid, yang merupakan jaringan listrik yang dilengkapi dengan teknologi informasi dan komunikasi untuk meningkatkan efisiensi, keandalan, dan keberlanjutan dalam penyediaan energi listrik. Dalam desain ini, beberapa komponen utama digunakan untuk memastikan operasional yang optimal. Berikut Spesifikasi komponen yang digunakan

3.1 Router

Device Name: Router2				
Device Model: Router-PT				
Hostname: Router				
Port	Link	IP Address	IPv6 Address	MAC Address
FastEthernet0/0	Up	192.168.1.1/24	<not set>	0050.0FCB.1B4A
FastEthernet1/0	Down	<not set>	<not set>	0090.2BA8.33E1
Serial2/0	Down	<not set>	<not set>	<not set>
Serial3/0	Down	<not set>	<not set>	<not set>
FastEthernet4/0	Down	<not set>	<not set>	0001.971E.2A24
FastEthernet5/0	Down	<not set>	<not set>	0060.5C00.60C1
Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Router2				

Gambar 2. Rancangan Router

Pada gambar 2 ditampilkan perangkat jaringan dengan nama Router2 yang merupakan bagian dari model perangkat Router-PT dan memiliki hostname Router. Perangkat ini memiliki beberapa port dengan status dan konfigurasi yang berbeda-beda. Port FastEthernet0/0 dalam keadaan aktif (Up) dengan alamat IP 192.168.1.1/24, sementara port lainnya seperti FastEthernet1/0, Serial2/0, Serial3/0, FastEthernet4/0, dan FastEthernet5/0 berada dalam keadaan tidak aktif (Down) dan belum dikonfigurasi alamat IP-nya. Alamat MAC yang terdaftar untuk setiap port juga berbeda, misalnya, FastEthernet0/0 memiliki alamat MAC 0050.0FCB.1B4A. Router ini berada di lokasi fisik Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Router2.

3.2 Laptop

Device Name: Laptop0				
Device Model: Laptop-PT				
Port	Link	IP Address	IPv6 Address	MAC Address
Wireless0	Up	169.254.114.105/16	<not set>	0090.2BB2.7269
Bluetooth	Down	<not set>	<not set>	0000.0C5E.6886
Gateway: <not set>				
DNS Server: <not set>				
Line Number: <not set>				
Wireless Best Data Rate: 54 Mbps				
Wireless Signal Strength: 100%				
Physical Location: Intercity > Home City > Corporate Office > Laptop0				

Gambar 3. Rancangan laptop

Gambar 3 merupakan Rancangan Laptop menunjukkan konfigurasi jaringan dari sebuah perangkat bernama "Laptop0" dengan model "Laptop-PT". Pada bagian port dan status link, terlihat bahwa port "Wireless0" sedang aktif dengan status "Up" dan memiliki alamat IP 169.254.114.105/16, namun tidak memiliki alamat IPv6 yang diset. Alamat MAC untuk port ini adalah 0090.2BB2.7269. Port "Bluetooth" sedang tidak aktif dengan status "Down" dan juga tidak memiliki alamat IP atau IPv6 yang diset, dengan alamat MAC 0000.0C5E.6886. Bagian gateway, DNS server, dan line number belum diatur, sehingga ditampilkan sebagai "<not set>". Koneksi nirkabel perangkat ini memiliki kecepatan data terbaik sebesar 54 Mbps dan kekuatan sinyal mencapai 100%. Terakhir, lokasi fisik dari perangkat ini digambarkan dengan hierarki "Intercity > Home City > Corporate Office > Laptop0". Informasi ini biasanya digunakan untuk mendiagnosis atau mengkonfigurasi koneksi jaringan perangkat tersebut. Adanya alamat IP 169.254.x.x menunjukkan bahwa perangkat tidak mendapatkan alamat IP dari server DHCP dan menggunakan alamat link-local otomatis, yang biasanya terjadi ketika perangkat gagal mendapatkan alamat IP dari jaringan.

3.3 Smartphone

Device Name: Smartphonel(3)				
Device Model: SMARTPHONE-PT				
Port	Link	IP Address	IPv6 Address	MAC Address
Wireless0	Up	169.254.113.41/16	<not set>	0090.21DC.7129
3G/4G Cell1	Up	<not set>	<not set>	0090.0C1B.057B
Bluetooth	Down	<not set>	<not set>	00E0.F9EB.BAD0
Gateway: <not set>				
DNS Server: <not set>				
Line Number: <not set>				
Wireless Best Data Rate: 54 Mbps				
Wireless Signal Strength: 69%				
Physical Location: Intercity > Home City > Corporate Office > Smartphonel(3)				

Gambar 4. Rancangan Smartphone

Gambar 3 merupakan Rancangan Smartphone menunjukkan konfigurasi jaringan dari sebuah perangkat bernama "Smartphone1" dengan model "SMARTPHONE-PT". Pada bagian port dan status link, terlihat bahwa port "Wireless0" sedang aktif dengan status "Up" dan memiliki alamat IP 169.254.113.41/16, namun tidak memiliki alamat IPv6 yang diset. Alamat MAC untuk port ini adalah 0090.21DC.7129. Port "Bluetooth" sedang tidak aktif dengan status "Down" dan juga tidak memiliki alamat IP atau IPv6 yang diset, dengan alamat MAC 0090.0CIB.0578. Bagian gateway, DNS server, dan line number belum diatur, sehingga ditampilkan sebagai "<not set>". Koneksi nirkabel perangkat ini memiliki kecepatan data terbaik sebesar 54 Mbps dan kekuatan sinyal mencapai 100%. Terakhir, lokasi fisik dari perangkat ini digambarkan dengan hierarki "Intercity > Home City > Corporate Office > Laptop0". Informasi ini biasanya digunakan untuk mendiagnosis atau mengkonfigurasi koneksi jaringan perangkat tersebut. Adanya alamat IP 169.254.x.x menunjukkan bahwa perangkat tidak mendapatkan alamat IP dari server DHCP dan menggunakan alamat link-local otomatis, yang biasanya terjadi ketika perangkat gagal mendapatkan alamat IP dari jaringan.

3.4 Access Point

```
Device Name: Access Point0
Device Model: AccessPoint-PT

Port      Link
Port 0    Up
Port 1    Up

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Access Point0
```

Gambar 5. Rancangan Accesspoint

Gambar ini menunjukkan konfigurasi jaringan untuk sebuah perangkat bernama "Access Point" dengan model "AccessPoint-PT". Perangkat ini memiliki dua port, yaitu Port 0 dan Port 1, yang keduanya berstatus "Up", menunjukkan bahwa kedua port tersebut aktif dan berfungsi dengan baik. Selain itu, informasi mengenai lokasi fisik perangkat juga disertakan dalam gambar ini. Lokasi fisik perangkat digambarkan dengan hierarki sebagai "Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Access Point0", yang memberikan detail spesifik tentang posisi perangkat dalam jaringan fisik. Informasi ini penting untuk keperluan manajemen dan pemeliharaan jaringan, memastikan bahwa teknisi dapat dengan mudah menemukan dan mengakses perangkat saat diperlukan.

3.5 PC

```
Device Name: PC4
Device Model: PC-PT

Port      Link      IP Address      IPv6 Address      MAC Address
FastEthernet0  Up      169.254.218.150/16 <not set>      00E0.F967.DA96
Bluetooth      Down      <not set>      <not set>      0001.633D.98B7

Gateway: <not set>
DNS Server: <not set>
Line Number: <not set>

Physical Location: Intercity > Home City > Corporate Office > PC4
```

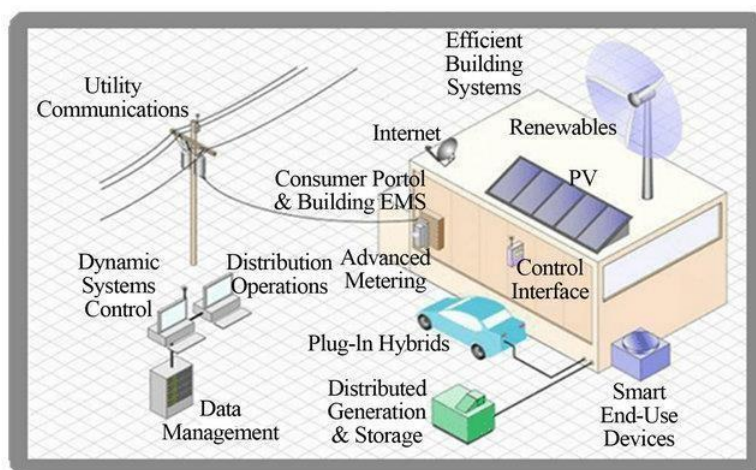
Gambar 6. Rancangan PC

Gambar ini memberikan informasi tentang konfigurasi jaringan dari sebuah perangkat bernama "PC4" dengan model "PC-PT". Perangkat ini memiliki dua port: "FastEthernet0" dan "Bluetooth". Port "FastEthernet0" berstatus "Up", artinya port ini aktif dan berfungsi, dengan alamat IP 169.254.218.150/16, tetapi tidak memiliki alamat IPv6 yang diset. Alamat MAC untuk port ini adalah 00E0.F967.DA96. Port "Bluetooth" berstatus "Down", artinya port ini tidak aktif, dan tidak memiliki alamat IP atau IPv6 yang diset. Alamat MAC untuk port ini adalah 0001.633D.98B7. Bagian gateway, DNS server, dan line number belum diatur, sehingga ditampilkan sebagai "<not set>". Terakhir, lokasi fisik perangkat ini dijelaskan dengan hierarki "Intercity > Home City > Corporate Office > PC4", memberikan detail spesifik tentang posisi perangkat dalam jaringan fisik. Informasi ini penting untuk manajemen dan pemeliharaan jaringan, memastikan teknisi dapat dengan mudah menemukan dan mengakses perangkat saat diperlukan. Adanya alamat IP 169.254.x.x menunjukkan bahwa perangkat tidak mendapatkan alamat IP dari server DHCP dan menggunakan alamat link-local otomatis, yang biasanya terjadi ketika perangkat gagal mendapatkan alamat IP dari jaringan.

Hasil implementasi menunjukkan bahwa dengan adanya sistem keamanan berlapis dan penggunaan teknologi canggih, Smart Grid dapat beroperasi dengan aman dan efisien. Evaluasi melalui pengujian penetrasi dan analisis kinerja menunjukkan bahwa sistem yang dirancang mampu mendeteksi dan mencegah berbagai ancaman siber, memastikan integritas, kerahasiaan, dan ketersediaan data serta operasional Smart Grid.

Implementasi sistem keamanan jaringan Smart Grid memerlukan pendekatan yang terstruktur dan bertahap. Langkah pertama adalah melakukan analisis kebutuhan yang komprehensif, mencakup identifikasi aset-aset kritis, potensi ancaman, dan kerentanan jaringan. Berdasarkan analisis ini, rencana keamanan yang terperinci dikembangkan, meliputi strategi mitigasi risiko, kebijakan keamanan, dan prosedur operasional. Arsitektur keamanan yang dirancang harus mencakup berbagai lapisan perlindungan, seperti perlindungan perimeter menggunakan firewall dan IDS/IPS, segmentasi jaringan untuk keamanan internal, enkripsi data untuk perlindungan data, serta sistem otentikasi dan otorisasi untuk memastikan akses yang sah. Selain itu, pemantauan dan audit real-time juga diperlukan untuk mendeteksi aktivitas mencurigakan.

Setelah perencanaan, komponen utama sistem keamanan dikembangkan dan diintegrasikan ke dalam jaringan Smart Grid. Ini mencakup konfigurasi firewall, IDS/IPS, implementasi protokol enkripsi seperti TLS/SSL, dan penggunaan metode otentikasi multifaktor. Pengujian menyeluruh dilakukan untuk memastikan semua komponen berfungsi dengan baik dan mampu menghadapi ancaman keamanan diberikan kepada personel yang akan mengoperasikan sistem, serta dokumentasi lengkap disediakan untuk memastikan pemahaman yang jelas tentang pengelolaan sistem. Pemantauan berkelanjutan dan pemeliharaan rutin juga penting untuk memastikan sistem tetap up-to-date dengan ancaman terbaru dan berfungsi optimal. Implementasi yang efektif memastikan bahwa jaringan Smart Grid dapat beroperasi dengan aman dan andal, melindungi aset-aset kritis, serta meminimalkan risiko dari ancaman keamanan siber



Gambar 7. Model dan scenario smart grid oleh EPRI

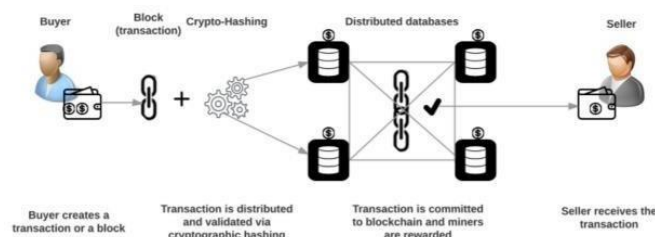
Gambar tersebut menggambarkan sebuah sistem Smart Grid yang mengintegrasikan berbagai komponen untuk menciptakan jaringan listrik yang efisien, aman, dan andal. Smart Grid memanfaatkan teknologi informasi dan komunikasi untuk mengoptimalkan produksi, distribusi, dan konsumsi energi. Beberapa komponen utama yang terlihat pada gambar ini meliputi sistem komunikasi utilitas, sistem kontrol dinamis, manajemen data, operasi distribusi, dan metering canggih. Sistem komunikasi utilitas memastikan aliran informasi yang cepat dan efisien antara berbagai komponen jaringan. Sistem kontrol dinamis memungkinkan penyesuaian real-time berdasarkan kondisi jaringan, sedangkan manajemen data mengumpulkan, menganalisis, dan mengarsipkan informasi penting untuk pengambilan keputusan yang lebih baik.

gambar ini juga menunjukkan pentingnya integrasi sumber energi terbarukan seperti panel surya (PV) dan sistem energi angin, yang dikendalikan oleh antarmuka kontrol. Energi terbarukan ini tidak hanya membantu mengurangi ketergantungan pada bahan bakar fosil tetapi juga mendukung keberlanjutan lingkungan. Sistem manajemen energi bangunan (EMS) dan portal konsumen memungkinkan pemilik bangunan untuk memantau dan mengelola konsumsi energi mereka secara efisien. Sistem metering canggih menyediakan data yang akurat tentang penggunaan energi, membantu dalam mengidentifikasi peluang penghematan energi. Kendaraan hibrida plug-in dan perangkat end-use pintar juga merupakan bagian dari ekosistem Smart Grid, yang memungkinkan penyimpanan dan penggunaan energi yang lebih fleksibel.

Implementasi sistem Smart Grid ini memerlukan infrastruktur yang kuat dan integrasi teknologi yang cermat. Distribusi generasi dan penyimpanan energi memastikan bahwa energi yang dihasilkan dari sumber terbarukan dapat disimpan dan digunakan sesuai kebutuhan. Sistem ini juga memungkinkan respon dinamis terhadap permintaan energi, sehingga meningkatkan efisiensi operasional dan mengurangi beban puncak. Secara keseluruhan, Smart Grid menawarkan solusi yang lebih canggih dan efisien untuk manajemen energi, dengan kemampuan untuk mengintegrasikan berbagai sumber energi, meningkatkan keamanan jaringan, dan memberikan kontrol yang lebih baik kepada pengguna akhir. Implementasi yang sukses dari sistem ini dapat mengarah pada jaringan listrik yang lebih stabil, berkelanjutan, dan ekonomis.

Blockchain adalah sebuah teknologi yang memungkinkan penyimpanan data secara aman, transparan, dan terdesentralisasi. Secara sederhana, blockchain adalah sebuah rantai blok data yang terhubung satu sama lain menggunakan kriptografi. Setiap blok dalam blockchain berisi sejumlah data transaksi yang telah diverifikasi dan dicatat secara permanen. Blok-blok ini disusun secara kronologis, sehingga setiap blok baru selalu ditambahkan di akhir rantai.

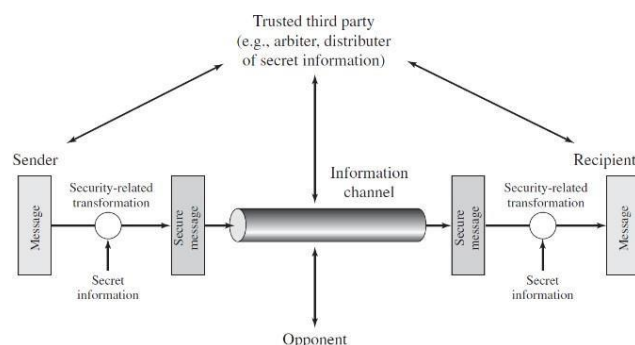
Blockchain - Process



Gambar 8. Proses Blockchain

Blockchain dapat diasumsikan sebagai arsip transaksi yang dikumpulkan pada blok-blok dengan penanda waktu atau timestamp. Setiap blok juga teridentifikasi dengan suatu nilai hash. Namun, setiap blok tersebut mereferensikan nilai hash dari blok yang ada sebelumnya. Fungsi hash merupakan suatu fungsi matematika yang mengambil masukan panjang variabel dan mengubahnya ke dalam urutan biner dengan panjang yang tetap. Fungsi ini digunakan pada berbagai aplikasi pengamanan dan protokol internet. Beberapa contoh kegunaannya adalah untuk autentikasi pesan, tanda tangan digital, dan penyimpanan password.

Kriptografi dalam konteks keamanan jaringan Smart Grid penting untuk melindungi data yang dikirimkan dan diterima di dalam sistem. Ini meliputi penggunaan teknik enkripsi untuk mengamankan informasi dari akses tidak sah, serta untuk memastikan otentikasi dan integritas data yang dikirimkan di seluruh jaringan. Dengan menerapkan kriptografi yang kuat, Smart Grid dapat memastikan bahwa informasi sensitif seperti penggunaan energi dan kontrol jaringan tidak dapat diakses atau dimodifikasi oleh pihak yang tidak berwenang, menjaga keamanan dan keandalan operasional sistem secara keseluruhan.



Gambar 9. Proses Kriptografi

Kriptografi dalam penerapan keamanan jaringan Smart Grid melibatkan penggunaan teknik enkripsi untuk melindungi data sensitif yang dikirim dan diterima di dalam sistem. Enkripsi memastikan bahwa informasi seperti data penggunaan energi atau instruksi pengendalian tidak dapat diakses oleh pihak yang

tidak sah. Selain itu, kriptografi juga mencakup otentikasi, yang memverifikasi identitas pengirim dan penerima data, serta memastikan integritas data dengan menggunakan metode seperti checksum atau hash untuk mendeteksi perubahan yang tidak sah. Teknik non-repudiasi juga diterapkan untuk mencegah pengirim menyangkal pengiriman pesan atau transaksi yang telah mereka lakukan. Dengan menerapkan kriptografi secara efektif, Smart Grid dapat menjaga keamanan dan keandalan operasional sistem, serta melindungi informasi penting dari ancaman peretasan atau manipulasi data di dalam jaringan energi yang semakin terhubung dan kompleks.

4. KESIMPULAN DAN SARAN

Dalam konteks keamanan jaringan Smart Grid, penelitian ini berhasil merancang dan mengimplementasikan sistem keamanan yang efektif untuk melindungi infrastruktur kritis dari ancaman siber. Metodologi yang digunakan meliputi analisis risiko, pengembangan model ancaman, dan penerapan teknologi keamanan canggih seperti enkripsi dan otentikasi multifaktor. Sistem keamanan yang diusulkan mengintegrasikan berbagai lapisan perlindungan, termasuk firewall, sistem deteksi intrusi, dan protokol keamanan berbasis.

blockchain untuk menjaga integritas data. Hasil implementasi menunjukkan bahwa sistem ini mampu mengidentifikasi dan menangkal serangan dengan efektif, meningkatkan resiliensi jaringan terhadap ancaman. Pengujian performa juga menunjukkan bahwa meskipun ada penambahan lapisan keamanan, sistem tetap beroperasi dalam batasan yang dapat diterima untuk latency dan throughput.

Penelitian ini memberikan kontribusi penting dalam pengembangan standar keamanan untuk Smart Grid, menawarkan rekomendasi praktis untuk industri dalam merancang sistem keamanan yang andal dan efisien.

DAFTAR PUSTAKA

- [1] Ashilah Aspiani Putri, Rahman Rakhmadi (2024). FORENSIK JARINGAN UNTUK INVESTIGASI KEJAHATAN CYBER PADA STUDI KASUS PEMBOBOLAN DATA KOMINFO OLEH BJORKA. (2024). *Jurnal Riset Sistem Informasi*, 1(3), 17-26. <https://doi.org/10.69714/g2pay047>
- [2] Anderson, R. (2001). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley.
- [3] Eka Putra R Palaloi Rahmat, Rahman Rakhmadi (2024). ANALISIS DAN PENCEGAHAN SERANGAN SOSIAL ENGINEERING PADA JARINGAN KOMPUTER STUDI KASUS PENIPUAN INVESTASI CRYPTO. (2024). *Jurnal Riset Sistem Informasi*, 1(3), 08-16. <https://doi.org/10.69714/8b7xtv35>
- [4] EPRI (Electric Power Research Institute). (2020). *Smart Grid Cybersecurity: Challenges and Solutions*. EPRI Journal.
- [5] Fendi Prasetyo Syaifudin, Feri Efendi Tino, Muqorobin (2024). IMPLEMENTASI SISTEM PREDIKSI CURAH HUJAN DENGAN PENERAPAN JARINGAN SYARAF TIRUAN BERBASIS WEBSITE. (2024). *Jurnal Riset Teknik Komputer*, 1(2), 80-96. <https://doi.org/10.69714/gn6nym06>
- [6] Farhangi, H. (2010). The path of the smart grid. *IEEE Power and Energy Magazine*.
- [7] Metke, A. R., & Ekl, R. L. (2010). Security technology for smart grid networks. *IEEE Transactions on Smart Grid*.
- [8] Mo, Y., Kim, T. H. J., Brancik, K., Dickinson, D., Lee, H., Perrig, A., & Sinopoli, B. (2012). Cyber– physical security of a smart grid infrastructure. *Proceedings of the IEEE. Approach for Higher Education. International Journal of Gaming and Computer-Mediated Simulations*, 9(1), 52-65.
- [9] Muhammad Alfian , Rahman Rakhmadi (2024). KEAMANAN JARINGAN PADA PERGURUAN TINGGI. (2024). *Jurnal Riset Sistem Informasi*, 1(3), 59-64. <https://doi.org/10.69714/qgnbgv11>
- [10] Yulhendri, Y., Simorangkir, H., Faridho, F., & Kurniawan, D. (2022). Implementasi Digital Dashboard Untuk Mengontrol Wilayah Rt/Rw. *Jurnal Informatika Dan Teknologi Komputer (JITEK)*, 2(1), 43-54.